A THEOREM ON DIOPHANTINE APPROXIMATION

by

N.G. de Bruijn

Eindhoven University of Technology
Dept. of Mathematics and Computing Science
PO Box 513, 5600MB Eindhoven, The Netherlands
A theorem on Diophantine approximation

by N.G. de Bruijn

1. Notation.

If m and n are positive integers then $M(m,n)$ is the set of all matrices with m rows and n columns.

The set of all real column vectors of length m is denoted as $R(m)$; it can be identified with $M(m,1)$. Furthermore, $Z(m)$ is the subset of $R(m)$ consisting of all vectors with integral entries.

The length of a vector $x$ is always denoted by $|x|$. If $B \in M(m,n)$ then $|B|$ denotes the maximum of $|Bx|$ for all $x \in R(n)$ with $|x| = 1$.

The transpose of a matrix $A$ will be written as $A^T$.

2. The main theorem.

Among the various equivalent forms we select as our main theorem.

Theorem 2.1. Let m and n be positive integers, and let $A \in M(m,m)$, $B \in M(m,n)$. Assume that $A$ is non-singular. Then for every positive number $\varepsilon$ there exists a positive number $\theta$ such that for every $c \in R(n)$ there exists an $x \in Z(n)$ and a $z \in Z(m)$ such that

$$|Bx - Az| < \varepsilon \quad \text{and} \quad |x - c| < \theta.$$ 

We shall show that the theorem is equivalent to theorem 3.2,
and that one will be proved in section 4.

3. Equivalent forms.

Theorem 3.1. As theorem 2.1, but with "$x \in Z(n)$" replaced by "$x \in \mathbb{R}(n)$".

This is obviously a special case of theorem 2.1, but we show how theorem 2.1 follows from this special case. We apply theorem 3.1 with $m$ replaced by $m + n$, $A$ and $B$ by

$$
\begin{pmatrix}
A & 0 \\
0 & I
\end{pmatrix} \quad \text{and} \quad 
\begin{pmatrix}
B \\
I
\end{pmatrix},
$$

respectively, where $I$ is the unit matrix in $M(n,n)$. Now theorem 3.1 shows that for every $c \in \mathbb{R}(n)$ there exists an $x \in Z(n)$ and $z_1 \in Z(m)$, $z_2 \in Z(n)$ such that $|x - c| < \varepsilon$ and

$$
|Bx - Az_1| < \varepsilon, \quad |x - z_2| < \varepsilon.
$$

So $z_1$ and $z_2$ satisfy

$$
|Bz_2 - Az_1| < \varepsilon + |B| \varepsilon, \quad |z_2 - c| < \varepsilon + \varepsilon.
$$

Now theorem 2.1 follows by means of trivial adaptations of $\varepsilon$ and $\rho$.

Theorem 3.2. As theorem 3.1, but with $A$ replaced by the unit matrix $I$.

This is obviously equivalent to theorem 3.1. Note
that if $|A^{-1}Bx - z| < \varepsilon / |A|$ then $|Bx - Az| < \varepsilon$.

4. Proof of theorem 3.2.

We present two proofs. The first one is fast, but depends on the theory of almost periodic functions. The second one can be considered as more direct. It will be presented in all detail.

First proof. We use almost periodic functions of a vector variable (see Besicovitch [1], ch. 1.12).

If the rows of $B$ are $b_1^T, ..., b_m^T$, then

$$
\hat{\psi}(x) = \sum_{1 \leq j \leq m} \cos(2\pi (b_j^T x))
$$

is defined for all $x \in \mathbb{R}(n)$. As a sum of periodic functions it is uniformly almost periodic. So if $\varepsilon > 0$, the set of all $x \in \mathbb{R}(n)$ with $|\hat{\psi}(x) - m| < \varepsilon$ is relatively dense, i.e., there exists a $\varepsilon > 0$ such that for every $c \in \mathbb{R}(n)$ there exists an $x \in \mathbb{R}(n)$ with $|x - c| < \varepsilon$, $|\hat{\psi}(x) - m| < \varepsilon$.

The latter inequality is easily interpreted as the statement that all the entries of the column vector $Bx$ are close to an integer.

Second proof. Let $V$ be the set of all $Bx$ with $x \in \mathbb{R}(n)$. Let $W$ be the orthogonal complement of $V$ in $\mathbb{R}(m)$. The orthogonal projection operators onto $V$ and $W$ will be denoted by $P_V$ and $P_W$, respectively.

Let $S$ be the set of all $P_W z$ with $z \in \mathbb{Z}(m)$, and $T$ the set of all $w \in W$ with $|w| \leq m^\gamma$.

Let $\varepsilon$ be a positive number. We can cover the closure of $S \cap T$ by means of the set of all open spheres with center in $S \cap T$.
and with radius $\xi$. Since that closure is compact, we can find a finite subset $Y$ of $S \cap T$ such that every point of $S \cap T$ has distance less than $\xi$ to $Y$. Every element of $Y$ has the form $P_W z$ with $z \in Z(m)$, so we can find a finite subset $Q$ of $Z(m)$ such that for every $z \in Z(m)$ with $|P_W z| \leq m^{\nu}$ there exists a point $q \in Q$ with $|P_W z - P_W q| < \xi$.

By $\omega$ we denote the maximum of $|q|$ when $q$ runs through the finite set $Q$.

As a last preparation we mention that there exists a positive number $\sigma^-$ such that for every $v \in V$ there is a $y \in R(n)$ with $By = v$ and $|y| \leq \sigma |v|$. This is trivial if $B$ is a projection operator, and the general case can be reduced to this one by multiplication with non-singular matrices on the left as well as on the right.

We are now ready for the proof. We take $\rho = (m^{\nu} + \omega^-) \sigma^-$. Let $c \in R(n)$ be arbitrary. We can fix $z_o \in Z(m)$ such that $|z_o - Bc| \leq m^{\nu}$. Hence $|P_W z_o| \leq m^{\nu}$. So we can take $q \in Q$ with $|P_W z_o - P_W q| < \xi$.

We note that $|q| \leq \omega^-$. We have $P_V (z_o - q - Bc) \in V$, so we can fix $y \in R(n)$ with $P_V (z_o - q - Bc) = By$ and

$$|y| \leq \sigma |P_V (z_o - q - Bc)| \leq \sigma |z_o - q - Bc| \leq \sigma (m^{\nu} + \omega^-) = \rho^-.$$

We can now fix $x$ and $z$:

$$x = c + y, \quad z = z_o - q,$$

so indeed $x \in R(n)$, $z \in Z(m)$ and $|x - c| \leq \rho^-$. We finally have to show $|Bx - z| < \xi$. We have

$$Bx = Bc + By = P_V Bc + By = P_V (z_o - q),$$
whence
\[ |Bx - z| \leq |P (z - q) - (z_q - q)| = |P (z - q)| < \varepsilon. \]

This finishes the proof.

5. Extension to infinite dimensional spaces.

The technique of the second proof of section 4 can be applied at once to prove a theorem on (possibly infinite dimensional) normed real linear spaces.

If in such a space \( R \) we have a subset \( S \) and if \( \alpha > 0 \) then the notation \( \text{nb}(S, \alpha) \) is used for the \( \alpha \)-neighborhood of \( S \), i.e., the set of all \( r \in R \) with distance less than \( \alpha \) to \( S \).

If there exists a \( \rho > 0 \) such that \( \text{nb}(S, \rho) = R \) then we say that \( S \) is relatively dense in \( R \).

**Theorem 5.1.** Let \( R \) be a normed real linear space, and let \( Z \) be a subgroup of \( R \) under addition. Let \( V \) be a linear subspace of \( R \) such that the factor space \( R/V \) has finite dimension. Assume that \( \rho > 0 \) exists such that \( \text{nb}(Z, \rho) \supset V \) (in particular this is true if \( Z \) is relatively dense in \( R \)). Then for every \( \varepsilon > 0 \) the intersection \( \text{nb}(Z, \varepsilon) \cap V \) is relatively dense in \( V \).

6. Application to almost periodicity.

The first proof of section 4 depended on the theory of almost periodic functions. We now proceed in an opposite direction, by
showing that the method of the second proof of section 4 can be used as a tool to support that theory of almost periodic functions.

A continuous mapping of \( R(m) \) into some normed linear space is called uniformly almost periodic (u.a.p.) if for every \( \varepsilon > 0 \) the set of translation vectors belonging to \( \varepsilon \) is relatively dense. The notion "relatively dense" was explained in section 5; a "translation vector belonging to \( \varepsilon \)" is a vector \( b \in R(m) \) with the property that 

\[
|f(x + b) - f(x)| < \varepsilon \text{ for all } x \in R(m).
\]

Let \( M(\varepsilon) \) denote the set of all translation vectors belonging to \( \varepsilon \). Then we have the following properties:

(i) For every \( \varepsilon > 0 \) the origin \( 0 \) is an interior point of \( M(\varepsilon) \).

(ii) For every \( \varepsilon > 0 \) there exists a \( \delta > 0 \) such that for all \( x, y \) with \( x \in M(\delta), y \in M(\delta) \) we have \( x + y \in M(\varepsilon), x - y \in M(\varepsilon) \).

(iii) For all \( \varepsilon, \delta \) with \( 0 < \varepsilon < \delta \) we have \( M(\varepsilon) \subseteq M(\delta) \).

By the method of the second proof of section 4 we can establish the following theorem:

**Theorem 6.1.** Let \( R \) be a normed real linear space, and let \( V \) be a linear subspace such that the factor space \( R/V \) has finite dimension. Let \( M(\alpha) \) be a subset of \( R \), for every positive \( \alpha \). We assume that \( M(\alpha) \) satisfies conditions (i), (ii) and (iii). Furthermore we assume that to every positive number \( \alpha \) there exists a positive number \( \varepsilon \) such that for every \( y \in V \) there exists \( z \in M(\alpha) \) with \( |z - y| < \varepsilon \) (in particular this is true if for every \( \alpha \) the set \( M(\alpha) \) is relatively dense in \( R \)). Then for every \( \varepsilon > 0 \) the intersection \( M(\alpha) \cap V \) is relatively dense in \( V \).

As an application we take two systems of sets \( M(\alpha) \) and
$M_1(\alpha)$, both relatively dense in $R(m)$ for all $\alpha > 0$, and both satisfying conditions (i)-(iii). We conclude that the system $M_1(\alpha) \cap M_2(\alpha)$ is again relatively dense in $R(m)$. This can be shown by means of theorem 6.1 in the following way. Take the space $R = R(m) \times R(m)$, and the subsets

$$M(\alpha) = (M_1(\alpha) \times R(m)) \cap (R(m) \times M_2(\alpha)).$$

For $V$ we take the diagonal, i.e., the set of all points $(x, x)$ with $x \in R(m)$. Then theorem 6.1 can be applied at once.

In particular this shows that the sum (or the product) of two u.a.p. functions is again u.a.p.

7. Remarks.

(i) The word "Diophantine" in the title does not appear in the text of this note. The title has been chosen since the problem belongs in the area covered by [3].

(ii) Theorem 3.2 played a role in the author's paper [2], section 17. This note was written since the author liked to have a proof that did not depend on almost periodic functions.

References.


Cambridge University Press 1932.

2. N.G. de Bruijn. Quasicrystals and their Fourier transform.
